

## UNITED STATES DISTRICT COURT

for the  
Middle District of North Carolina

In the Matter of the Search of  
(Briefly describe the property to be searched  
or identify the person by name and address)

Toyota Yaris vehicle bearing North Carolina license plate  
ZYD5374 and Vehicle Identification Number  
JTDKT903095263488

Case No. 15 MJ 304

## APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

A white in color vehicle described as a model year 2009 Toyota Yaris bearing North Carolina license plate ZYD5374 and Vehicle Identification Number JTDKT903095263488.

located in the Middle District of North Carolina, there is now concealed (identify the person or describe the property to be seized):

Evidence of, instrumentalities used in committing, and fruits of the crime of 18 U.S.C. §§ 2252A(a)(5)(B) and (b)(2), all of which are more particularly described in Attachment B, attached hereto and made a part hereof.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;  
☒ contraband, fruits of crime, or other items illegally possessed;  
☒ property designed for use, intended for use, or used in committing a crime;  
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	Offense Description
18 U.S.C. §§ 2252A(a)(5)(B) and (b)(2)	possession of child pornography, knowing access, conspiracy to access, or attempted access with intent to view child pornography

The application is based on these facts:

- ☒ Continued on the attached sheet.  
☐ Delayed notice of        days (give exact ending date if more than 30 days:       ) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

  
Applicant's signature

Tara S. Cataldo, FBI Special Agent

Printed name and title

Sworn to before me and signed in my presence.

Date: 10/15/15

City and state: Greensboro, North Carolina

  
Judge's signature

L. Patrick Auld, United States Magistrate Judge

Printed name and title

**IN THE UNITED STATES DISTRICT COURT  
FOR THE MIDDLE DISTRICT OF NORTH CAROLINA**

IN THE MATTER OF THE SEARCH OF THE  
PREMISES LOCATED AT: 112 ODELL  
PLACE, APARTMENT 4, GREENSBORO,  
NORTH CAROLINA 27403

AND

THE VEHICLE: TOYOTA YARIS BEARING  
NORTH CAROLINA LICENSE PLATE  
ZYD5374 AND VEHICLE IDENTIFICATION  
NUMBER JTDKT903095263488

  
~~UNDER SEAL~~

Case No. \_\_\_\_\_

**AFFIDAVIT IN SUPPORT OF APPLICATION FOR SEARCH WARRANT**

**INTRODUCTION**

I, Tara S. Cataldo, being duly sworn, depose and state as follows:

1. I am a Special Agent (SA) of the Federal Bureau of Investigation (FBI), and have been since March of 2008. My initial training consisted of a twenty week FBI new agent course during which I received instruction on various aspects of federal investigations. In addition, I have received more than 350 hours of training related to computers and cyber matters, to include investigations of cyber crime. I am currently assigned to the Charlotte Division and stationed at the Greensboro Resident Agency. Prior to joining the FBI, I worked in law enforcement for over eight years as a police officer and sheriff's investigator. I have been the case agent or supporting agent in numerous investigations, including investigations involving child pornography, kidnapping, computer intrusion, and internet fraud. I have received training in the area of child pornography and child exploitation, and have had the opportunity to observe and review numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in all

forms of media including computer media. Moreover, I am a federal law enforcement officer who is engaged in enforcing the criminal laws, including 18 U.S.C. §§ 2251 and 2252A, and I am authorized by the Attorney General to request a search warrant.

2. I have probable cause to believe that contraband and evidence of a crime, fruits of a crime, and instrumentalities of violations of 18 U.S.C. §§ 2252A(a)(5)(B) and (b)(2) (possession of, knowing access, conspiracy to access, or attempted access with intent to view child pornography), are located at 112 Odell Place, Apartment 4, Greensboro, North Carolina 27403 (hereinafter the "SUBJECT PREMISES") and in a Toyota Yaris vehicle bearing North Carolina license plate ZYD5374 and Vehicle Identification Number JTDKT903095263488 (hereinafter the "SUBJECT VEHICLE"), which are both located in the Middle District of North Carolina. I submit this application and affidavit in support of a search warrant authorizing a search of the SUBJECT PREMISES as described in Attachment A and the SUBJECT VEHICLE, for the items described in Attachment B, both incorporated herein by reference. I request authority to search the SUBJECT PREMISES and SUBJECT VEHICLE for the items described in Attachment B, and to seize all items listed in Attachment B as contraband and instrumentalities, fruits, and evidence of crime.
3. The statements contained in this affidavit are based in part on: information provided by FBI Special Agents; written reports about this and other investigations that I have received, directly or indirectly, from other law enforcement agents, information gathered from the service of administrative subpoenas; the results of physical and electronic surveillance conducted by law enforcement agents; independent investigation and analysis by FBI agents/analysts and computer forensic professionals; and my experience, training and

background as a Special Agent with the FBI. Because this affidavit is being submitted for the limited purpose of securing authorization for the requested search warrant, I have not included each and every fact known to me concerning this investigation. Instead, I have set forth only the facts that I believe are necessary to establish the necessary foundation for the requested warrant.

#### **RELEVANT STATUTES**

4. This investigation concerns alleged violations of 18 U.S.C. §§ 2252A(a)(5)(B) and (b)(2) (possession of, knowing access, conspiracy to access, or attempted access with intent to view child pornography).
  - a. 18 U.S.C. §§ 2252A(a)(5)(B) and (b)(2) prohibits a person from knowingly possessing or knowingly accessing with intent to view, or attempting to do so, any material that contains an image of child pornography, as defined in 18 U.S.C. § 2256(8), that has been mailed, or shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means, including by computer, or that was produced using materials that have been mailed or shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.

## **DEFINITIONS**

5. The following definitions apply to this Affidavit and attachments hereto:

- a. “Bulletin Board” means an Internet-based website that is either secured (accessible with a password) or unsecured, and provides members with the ability to view postings by other members and make postings themselves. Postings can contain text messages, still images, video images, or web addresses that direct other members to specific content the poster wishes. Bulletin boards are also referred to as “internet forums” or “message boards.” A “post” or “posting” is a single message posted by a user. Users of a bulletin board may post messages in reply to a post. A message “thread,” often labeled a “topic,” refers to a linked series of posts and reply messages. Message threads or topics often contain a title, which is generally selected by the user who posted the first message of the thread. Bulletin boards often also provide the ability for members to communicate on a one-to-one basis through “private messages.” Private messages are similar to e-mail messages that are sent between two members of a bulletin board. They are accessible only by the user who sent/received such a message, or by the Website Administrator.
- b. “Chat” refers to any kind of communication over the Internet that offers a real-time transmission of text messages from sender to receiver. Chat messages are generally short in order to enable other participants to respond quickly and in a format that resembles an oral conversation. This feature distinguishes chatting from other text-based online communications such as Internet forums and email.
- c. “Child Erotica,” as used herein, means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not, in and of themselves, legally

obscene or that do not necessarily depict minors in sexually explicit conduct.

- d. “Child Pornography,” as used herein, is defined in 18 U.S.C. § 2256(8) as any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct.
- e. “Computer,” as used herein, is defined pursuant to 18 U.S.C. § 1030(e)(1) as “an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device.”
- f. “Computer Server” or “Server,” as used herein, is a computer that is attached to a dedicated network and serves many users. A web server, for example, is a computer which hosts the data associated with a website. That web server receives requests from a user and delivers information from the server to the user’s computer via the Internet. A domain name system (“DNS”) server, in essence, is a computer on the Internet that routes communications when a user types a domain name, such as [www.cnn.com](http://www.cnn.com), into his or her web browser. Essentially, the domain name must be translated into an Internet Protocol (“IP”) address so the computer hosting the web site may be located, and the DNS server provides this function.
- g. “Computer hardware,” as used herein, consists of all equipment which can receive,

capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including, but not limited to, central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices); peripheral input/output devices (including, but not limited to, keyboards, printers, video display monitors, and related communications devices such as cables and connections), as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including, but not limited to, physical keys and locks).

- h. “Computer software,” as used herein, is digital information which can be interpreted by a computer and any of its related components to direct the way they work. Computer software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.
- i. “Computer-related documentation,” as used herein, consists of written, recorded, printed, or electronically stored material which explains or illustrates how to configure or use computer hardware, computer software, or other related items.
- j. “Computer passwords, pass-phrases and data security devices,” as used herein, consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password or pass-phrase (a string of alpha-numeric characters) usually operates as a sort of digital key to “unlock” particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data

security software of digital code may include programming code that creates “test” keys or “hot” keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or “booby-trap” protected data to make it inaccessible or unusable, as well as reverse the process to restore it.

- k. “File Transfer Protocol” (“FTP”), as used herein, is a standard network protocol used to transfer computer files from one host to another over a computer network, such as the Internet. FTP is built on client-server architecture and uses separate control and data connections between the client and the server.
- l. “Host Name,” as used herein, is a name assigned to a device connected to a computer network that is used to identify the device in various forms of electronic communication, such as communications over the Internet;
- m. “Hyperlink” refers to an item on a web page which, when selected, transfers the user directly to another location in a hypertext document or to some other web page.
- n. The “Internet” is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.
- o. “Internet Service Providers” (“ISPs”), as used herein, are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, e-mail, remote storage, and co-location of computers and other communications equipment. ISPs can offer a range of options in providing access to the Internet including telephone



based dial-up, broadband based access via digital subscriber line (“DSL”) or cable television, dedicated circuits, or satellite based subscription. ISPs typically charge a fee based upon the type of connection and volume of data, called bandwidth, which the connection supports. Many ISPs assign each subscriber an account name – a username or screen name, an "e-mail address," an e-mail mailbox, and a personal password selected by the subscriber. By using a computer equipped with a modem, the subscriber can establish communication with an Internet Service Provider (“ISP”) over a telephone line, through a cable system or via satellite, and can access the Internet by using his or her account name and personal password.

- p. “Internet Protocol address” or “IP address” refers to a unique number used by a computer to access the Internet. IP addresses can be “dynamic,” meaning that the ISP assigns a different unique number to a computer every time it accesses the Internet. IP addresses might also be “static,” if an ISP assigns a user’s computer a particular IP address which is used each time the computer accesses the Internet. IP addresses are also used by computer servers, including web servers, to communicate with other computers.
- q. Media Access Control (“MAC”) address. The equipment that connects a computer to a network is commonly referred to as a network adapter. Most network adapters have a MAC address assigned by the manufacturer of the adapter that is designed to be a unique identifying number. A unique MAC address allows for proper routing of communications on a network. Because the MAC address does not change and is intended to be unique, a MAC address can allow law enforcement to identify whether communications sent or received at different times are associated with the same adapter.

- r. “Minor” means any person under the age of eighteen years. See 18 U.S.C. § 2256(1).
- s. The terms “records,” “documents,” and “materials,” as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, painting), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies), mechanical form (including, but not limited to, phonograph records, printing, typing) or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMs, digital video disks (“DVDs”), Personal Digital Assistants (“PDAs”), Multi Media Cards (“MMCs”), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).
- t. “Secure Shell” (“SSH”), as used herein, is a security protocol for logging into a remote server. SSH provides an encrypted session for transferring files and executing server programs.
- u. “Sexually explicit conduct” means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any person. See 18 U.S.C. § 2256(2).
- v. “URL” is an abbreviation for Uniform Resource Locator and is another name for a web address. URLs are made of letters, numbers, and other symbols in a standard form.

People use them on computers by clicking a pre-prepared link or typing or copying and pasting one into a web browser to make the computer fetch and show some specific resource (usually a web page) from another computer (web server) on the Internet.

- w. “Visual depictions” include undeveloped film and videotape, and data stored on computer disk or by electronic means, which is capable of conversion into a visual image. See 18 U.S.C. § 2256(5).
- x. “Website” consists of textual pages of information and associated graphic images. The textual information is stored in a specific format known as Hyper-Text Mark-up Language (“HTML”) and is transmitted from web servers to various web clients via Hyper-Text Transport Protocol (“HTTP”).

### **BACKGROUND OF THE INVESTIGATION AND PROBABLE CAUSE**

- 6. A user of the Internet account at the SUBJECT PREMISES has been linked to an online community of individuals who regularly send and receive child pornography via a website that operated on an anonymous online network. The website is described below and referred to herein as “Website A.”<sup>1</sup> There is probable cause to believe that a user of the Internet account at the SUBJECT PREMISES knowingly accessed with intent to view child pornography on “Website A.”

---

<sup>1</sup> The actual name of “Website A” is known to law enforcement. Disclosure of the name of the site would potentially alert its members to the fact that law enforcement action is being taken against the site and its users, potentially provoking members to notify other members of law enforcement action, flee, and/or destroy evidence. Accordingly, for purposes of the confidentiality and integrity of the ongoing investigation involved in this matter, specific names and other identifying factors have been replaced with generic terms and the website will be identified as “Website A.”

## The Network<sup>2</sup>

7. “Website A” operated on a network (“the Network”) available to Internet users who are aware of its existence. The Network is designed specifically to facilitate anonymous communication over the Internet. In order to access the Network, a user must install computer software that is publicly available, either by downloading software to the user’s existing web browser, downloading free software available from the Network’s administrators, or downloading a publicly-available third-party application.<sup>3</sup> Using the Network prevents someone attempting to monitor an Internet connection from learning what sites a user visits and prevents the sites the user visits from learning the user’s physical location. Because of the way the Network routes communication through other computers, traditional IP identification techniques are not viable.
8. Websites that are accessible only to users within the Network can be set up within the Network. “Website A” was one such website. Accordingly, “Website A” could not generally be accessed through the traditional Internet.<sup>4</sup> Only a user who had installed the appropriate software on the user’s computer could access “Website A.” Even after connecting to the Network, however, a user had to know the exact web address of “Website A” in order to access it. Websites on the Network are not indexed in the same way as websites on the

---

<sup>2</sup> The actual name of the Network is known to law enforcement. The network remains active and disclosure of the name of the network would potentially alert its members to the fact that law enforcement action is being taken against the network, potentially provoking members to notify other members of law enforcement action, flee, and/or destroy evidence. Accordingly, for purposes of the confidentiality and integrity of the ongoing investigation involved in this matter, specific names and other identifying factors have been replaced with generic terms and the network will be identified as “the Network.”

<sup>3</sup> Users may also access the Network through so-called “gateways” on the open Internet, however, use of those gateways does not provide users with the full anonymizing benefits of the Network.

<sup>4</sup> Due to a misconfiguration, prior to February 20, 2015, Website A was occasionally accessible through the traditional Internet. In order to access Website A in that manner, however, a user would have had to know the exact IP address of the computer server that hosted Website A, which information was not publicly available. As of on or about February 20, 2015, Website A was no longer accessible through the traditional Internet.

traditional Internet. Accordingly, unlike on the traditional Internet, a user could not simply perform a Google search for the name of “Website A,” obtain the web address for “Website A,” and click on a link to navigate to “Website A.” Rather, a user had to have obtained the web address for “Website A” directly from another source, such as other users of “Website A,” or from online postings describing both the sort of content available on “Website A” and its location. Accessing “Website A” therefore required numerous affirmative steps by the user, making it extremely unlikely that any user could have simply stumbled upon “Website A” without first understanding its content and knowing that its primary purpose was to advertise and distribute child pornography.

9. The Network’s software protects users’ privacy online by bouncing their communications around a distributed network of relay computers run by volunteers all around the world, thereby masking the user’s actual IP address which could otherwise be used to identify a user.
10. The Network also makes it possible for users to hide their locations while offering various kinds of services, such as web publishing, forum/website hosting, or an instant messaging server. Within the Network itself, entire websites can be set up which operate the same as regular public websites with one critical exception - the IP address for the web server is hidden and instead is replaced with a Network-based web address. A user can only reach such sites if the user is using the Network client and operating in the Network. Because neither a user nor law enforcement can identify the actual IP address of the web server, it is not possible to determine through public lookups where the computer that hosts the website is located. Accordingly, it is not possible to obtain data detailing the activities of the users

from the website server through public lookups.

Description of “Website A” and its Content

11. “Website A” was a child pornography bulletin board and website dedicated to the advertisement and distribution of child pornography and the discussion of matters pertinent to the sexual abuse of children, including the safety and security of individuals who seek to sexually exploit children online. On or about February 20, 2015, the computer server hosting “Website A” was seized from a web-hosting facility in Lenoir, North Carolina. The website operated in Newington, Virginia, from February 20, 2015, until March 4, 2015, at which time “Website A” ceased to operate. Between February 20, 2015, and March 4, 2015, law enforcement agents acting pursuant to an order of the United States District Court for the Eastern District of Virginia monitored electronic communications of users of “Website A.” Before, during, and after its seizure by law enforcement, law enforcement agents viewed, examined and documented the contents of “Website A,” which are described below.
12. According to statistics posted on the site, “Website A” contained a total of 117,773 posts, 10,622 total topics, and 214,898 total members as of March 4, 2015. The website appeared to have been operating since approximately August 2014, which is when the first post was made on the message board. On the main page of the site, located to either side of the site name were two images depicting partially clothed prepubescent girls with their legs spread apart, along with the text underneath stating, “No cross-board reposts, .7z preferred, encrypt filenames, include preview, Peace out.” Based on my training and experience, I know that: “no cross-board reposts” refers to a prohibition against material that is posted on other websites from being “re-posted” to “Website A;” and “.7z” refers to a preferred method of

compressing large files or sets of files for distribution. Two data-entry fields with a corresponding "Login" button were located to the right of the site name. Located below the aforementioned items was the message, "Warning! Only registered members are allowed to access the section. Please login below or 'register an account' [(a hyperlink to the registration page)] with "[Website A]." Below this message was the "Login" section, consisting of four data-entry fields with the corresponding text, "Username, Password, Minutes to stay logged in, and Always stay logged in."

13. Upon accessing the "register an account" hyperlink, there was a message that informed users that the forum required new users to enter an email address that looks to be valid. However, the message instructed members not to enter a real email address. The message further stated that once a user registered (by selecting a username and password), the user would be able to fill out a detailed profile. The message went on to warn the user "[F]or your security you should not post information here that can be used to identify you." The message further detailed rules for the forum and provided other recommendations on how to hide the user's identity for the user's own security.
14. After accepting the above terms, registration to the message board then required a user to enter a username, password, and e-mail account; although a valid e-mail account was not required as described above.
15. After successfully registering and logging into the site, the user could access any number of sections, forums, and sub-forums. Some of the sections, forums, and sub-forums available to users included: (a) How to; (b) General Discussion; (c) [Website A] information and rules; and (d) Security & Technology discussion. Additional sections, forums, and sub-forums

included (a) Jailbait – Boy; (b) Jailbait – Girl; (c) Preteen – Boy; (d) Preteen – Girl; (e) Pre-teen Videos – Girl HC; (f) Pre-teen Videos – Boys HC; (g) Toddlers; and (h) Kinky Fetish – Scat. Based on my training and experience, I know that “jailbait” refers to underage but post-pubescent minors; the abbreviation “HC” means hardcore (i.e., depictions of penetrative sexually explicit conduct); and “scat” refers to the use of feces in various sexual acts, watching someone defecating, or simply seeing the feces. An additional section and forum was also listed in which members could exchange usernames on a Network-based instant messaging service that I know, based upon my training and experience, to be commonly used by subjects engaged in the online sexual exploitation of children.

16. A review of the various topics within the above forums revealed each topic contained a title, the author, the number of replies, the number of views, and the last post. The “last post” section of a particular topic included the date and time of the most recent posting to that thread as well as the author. Upon accessing a topic, the original post appeared at the top of the page, with any corresponding replies to the original post included in the post thread below it. Typical posts appeared to contain text, images, thumbnail-sized previews of images, compressed files (such as Roshal Archive files, commonly referred to as “.rar” files, which are used to store and distribute multiple files within a single file), links to external sites, or replies to previous posts.
17. A review of the various topics within the “[Website A] information and rules,” “How to,” “General Discussion,” and “Security & Technology discussion” forums revealed that the majority contained general information in regards to the site, instructions and rules for how to post, and welcome messages between users.



18. A review of topics within the remaining forums revealed the majority contained discussions about, and numerous images that appeared to depict, child pornography and child erotica depicting prepubescent girls, boys, and toddlers. Examples of these are as follows:
- a. On February 3, 2015, a user posted a topic entitled “Buratino-06” in the forum “Pre-teen – Videos - Girls HC” that contained numerous images depicting child pornography of a prepubescent or early pubescent girl. One of these images depicted the girl being orally penetrated by the penis of a naked male;
  - b. On January 30, 2015, a user posted a topic entitled “Sammy” in the forum “Pre-teen – Photos – Girls” that contained hundreds of images depicting child pornography of a prepubescent girl. One of these images depicted the female being orally penetrated by the penis of a male; and
  - c. On September 16, 2014, a user posted a topic entitled “9yo Niece - Horse.mpg” in the “Pre-teen Videos - Girls HC” forum that contained four images depicting child pornography of a prepubescent girl and a hyperlink to an external website that contained a video file depicting what appeared to be the same prepubescent girl. Among other things, the video depicted the prepubescent female, who was naked from the waist down with her vagina and anus exposed, lying or sitting on top of a naked adult male, whose penis was penetrating her anus.
19. A list of members, which was accessible after registering for an account, revealed that approximately 100 users made at least 100 posts to one or more of the forums. Approximately 31 of these users made at least 300 posts. In total, “Website A” contained thousands of postings and messages containing child pornography images. Those images

included depictions of nude prepubescent minors lasciviously exposing their genitals or engaged in sexually explicit conduct with adults or other children.

20. “Website A” also included a feature referred to as “[Website A] Image Hosting.” This feature of “Website A” allowed users of “Website A” to upload links to images of child pornography that are accessible to all registered users of “Website A.” On February 12, 2015, an FBI Agent accessed a post on “Website A” titled “Giselita” which was created by a particular “Website A” user. The post contained links to images stored on “[Website A] Image Hosting.” The images depicted a prepubescent girl in various states of undress. Some images were focused on the nude genitals of a prepubescent girl. Some images depicted an adult male's penis partially penetrating the vagina of a prepubescent girl.
21. Text sections of “Website A” provided forums for discussion of methods and tactics to use to perpetrate child sexual abuse. For example, on January 8, 2015, a user posted a topic entitled “should i proceed?” in the forum “Stories - Non-Fiction” that contained a detailed accounting of an alleged encounter between the user and a 5 year old girl. The user wrote “...it felt amazing feeling her hand touch my dick even if it was through blankets and my pajama bottoms...” The user ended his post with the question, “should I try to proceed?” and further stated that the girl “seemed really interested and was smiling a lot when she felt my cock.” A different user replied to the post and stated, “...let her see the bulge or even let her feel you up...you don't know how she might react, at this stage it has to be very playful...”

Court Authorized Use of Network Investigative Technique

22. Websites generally have Internet Protocol (“IP”) address logs that can be used to locate and identify the site’s users. In such cases, after the seizure of a website whose users were

engaging in unlawful activity, law enforcement could review those logs in order to determine the IP addresses used by users of “Website A” to access the site. A publicly available lookup could then be performed to determine what Internet Service Provider (“ISP”) owned the target IP address. A subpoena could then be sent to that ISP to determine the user to which the IP address was assigned at a given date and time.

23. However, because of the Network software utilized by “Website A,” any such logs of user activity would contain only the IP addresses of the last computer through which the communications of “Website A” users were routed before the communications reached their destinations. The last computer is not the actual user who sent the communication or request for information, and it is not possible to trace such communications back through the Network to that actual user. Such IP address logs therefore could not be used to locate and identify users of “Website A.”

24. Accordingly, on February 20, 2015, the same date “Website A” was seized, the United States District Court for the Eastern District of Virginia authorized a search warrant to allow law enforcement agents to deploy a Network Investigative Technique (“NIT”) on “Website A” in an attempt to identify the actual IP addresses and other identifying information of computers used to access “Website A.” Pursuant to that authorization, between February 20, 2015, and approximately March 4, 2015, each time any user or administrator logged into “Website A” by entering a username and password, the FBI was authorized to deploy the NIT which would send one or more communications to the user’s computer. Those communications were designed to cause the user’s computer to deliver to a computer, known to or controlled by the government, data that would help identify the user’s computer, its location, other

information about the computer, and the user of the computer accessing "Website A." That data included: the computer's actual IP address, and the date and time that the NIT determined what that IP address was; a unique identifier generated by the NIT (e.g., a series of numbers, letters, and/or special characters) to distinguish the data from that of other computers; the type of operating system running on the computer, including type (e.g., Windows), version (e.g., Windows 7), and architecture (e.g., x 86); information about whether the NIT had already been delivered to the computer; the computer's Host Name; the computer's active operating system username; and the computer's MAC address.

User "canada\_dry" on "Website A"

25. According to data obtained from logs on "Website A," monitoring by law enforcement, and the deployment of a NIT, a user with the username "canada\_dry" engaged in activity on "Website A" as documented below.
26. The profile page of user "canada\_dry" indicated this user originally registered an account on "Website A" on February 22, 2015. Profile information on "Website A" contains information about that user's participation on the site, including statistical information about the user's posts to the site and a categorization of those posts. According to the statistics section of this user's profile, the user "canada\_dry" was actively logged into the website for a total of approximately thirty four (34) minutes between February 22, 2015, and March 4, 2015.
27. On February 23, 2015, at 00:20 UTC+5, the user "canada\_dry" accessed a thread entitled "12yo and dog" in the forum "Zoo" (identified by law enforcement as Thread ID 16361). The user's IP address was not captured. The first post within the thread contained multiple embedded images of child pornography including some depicting a dog with a child. One of

the images depicted a female child under the age of 12, nude from the waste-down, spreading her legs wide while touching her genitalia in a lascivious manner. The child appears to be applying peanut butter to her genitalia. In addition, numerous individuals accessing this thread added comments. They included the following:

- a. "big thank you for this amazing and beautiful dirty girl."
- b. "Great video a really good dog :);"
- c. "that girl is a future star :o."

28. On February 23, 2015, at 00:44 UTC+5, the user "canada\_dry" accessed a thread entitled "Lauri ~8yo 3 videos, tasting cum" in the forum "Girls HC" (identified by law enforcement as Thread ID 18579). The user's IP address was not captured. A post within the thread contained links to three videos and provided preview images of a female child under the age of ten giving fellatio to an adult male. In addition to the posted images, numerous individuals accessing this thread added comments to the post. They included the following:

- a. "What a trooper!"
- b. "She is a trooper indeed. She is hanging in there and smiling when it is finished but you can clearly see she doesn't like the cumshots."

29. On February 23, 2015, at 01:52 UTC+5, the user "canada\_dry" accessed a thread entitled "10 Great! Videos of FATTERMAN Collection (blowjob, taste of cum, lesbian, fuck)" in the forum "Girls HC" (identified by law enforcement as Thread ID 14317). The user's IP address was not captured. The first post within the thread contained multiple embedded images of child pornography. One of the images depicted three nude female children under the age of

12 displaying their genitalia. In addition, numerous individuals accessing this thread added comments. One individual posted the following: "WOW is there any more vid's of theses girls fucking and more sucking? Moreal she is da bomb. I wish I could find this little hottie during my travels in PI hehe.... any info PM me ;)."

30. A user activity report for "Website A" revealed that the user "canada\_dry" viewed nine threads located within "Website A." The titles of some of these threads were as follows:
- a. "Young girl playing with her dog;"
  - b. "The well known Polski girl and her dog (aka Obraz-series) pics and 1 small vid;"
  - d. "girl playing with a kitten;"
  - e. "Kenny Rogers FFFF (10-12yo) CAPS;"and
  - g. "Mask Girl German 12yo girl sucks daddy dick."

IP Address and Identification of User "canada\_dry" on "Website A"

31. According to data obtained from logs on "Website A," monitoring by law enforcement, and the deployment of a NIT, on March 4, 2015, at 20:28 UTC, the user "canada\_dry" accessed "Website A" from IP address 75.183.30.68. This user browsed "Website A" after logging in with a username and a password. At the time the user's IP address was captured, the name of the active operating system associated with the user's computer was revealed to be "i7PC" and the name of the active user account was "Admin."
32. On March 4, 2015, the user "canada\_dry" with IP address 75.183.30.38 accessed the thread entitled "My daughter 5yo - photo 2015" located in the forum "Girls HC" (identified by law enforcement as Thread ID 19998). This post contained numerous embedded images. The images were not recovered and thus I am not able to describe them. In addition to the posted

images, numerous individuals accessing this thread added comments. They included the following:

- a. "I'd love to see her face (though that's unsafe) and to se her penetrated, maybe a cumshot?"
- b. "she has nice feet. I could see more of it. and maybe footjob vid with cream on her pretty feet. Thnx." and
- c. "OMG!!! She is so much sexy! Can we see her suckin your dick?"

33. Using publicly available websites, FBI Special Agents were able to determine that the IP address 75.183.30.38 was operated by the Internet Service Provider ("ISP") Time Warner Cable on March 4, 2015.

34. On March 17, 2015, an administrative subpoena was served to Time Warner Cable requesting information related to the user who was assigned to the IP address 75.183.30.68. According to the information received from Time Warner Cable, Sawyer Beaton is receiving Internet service at the SUBJECT PREMISES with an activation date of August 22, 2012. Internet service was current in the name of Sawyer Beaton as of October 14, 2015, at the SUBJECT PREMISES.

35. On September 23, 2015, surveillance of the SUBJECT PREMISES revealed the property is in Guilford County, North Carolina. The SUBJECT PREMISES is located within 112 Odell Place, Greensboro, North Carolina 27403, which is described as a multi-family dwelling made of gray siding divided into at least seven apartments. The numbers "112" are located on the front porch post of the multi-family dwelling. All of the doors to the separate apartments in the multi-family dwelling are marked with their individual numbers. Access to the SUBJECT PREMISES is through the second door on the right when facing the house from

the street and up the stairs to the right, designated by the number 4 on the right doorjamb.

36. A search of Accurint and Clear databases (public records databases that provides names, dates of birth, addresses, associates, telephone numbers, email addresses, etc.) was conducted for the SUBJECT PREMISES. These public records indicated that the SUBJECT PREMISES is currently a residence of Ernest Sawyer Beaton, also known as Sawyer Beaton.
37. On October 2, 2015, the landlord of the SUBJECT PREMISES was contacted. He advised that the SUBJECT PREMISES was still occupied by Sawyer Beaton.
38. A check of the North Carolina Department of Motor Vehicles revealed that two vehicles are registered to Ernest Sawyer Beaton at a different address than the SUBJECT PREMISES. These two vehicles are a 2004 Toyota Corolla Matrix bearing North Carolina license plate YXP6192 and a 2009 Toyota Yaris bearing North Carolina license plate ZYD5374 (the SUBJECT VEHICLE). On October 8 and 14, 2015, surveillance revealed the SUBJECT VEHICLE parked directly across the street from the SUBJECT PREMISES.

### **BACKGROUND ON COMPUTERS AND CHILD PORNOGRAPHY**

39. Computers and digital technology have dramatically changed the way in which individuals interested in child pornography interact with each other. Computers basically serve four functions in connection with child pornography: production, communication, distribution, and storage.
40. Child pornographers can now transfer printed photographs into a computer-readable format with a device known as a scanner. Furthermore, with the advent of digital cameras, when the photograph is taken it is saved as a digital file that can be directly transferred to a computer



by simply connecting the camera to the computer. In the last ten years, the resolution of pictures taken by digital cameras has increased dramatically, meaning the photos taken with digital cameras have become sharper and crisper. Photos taken on a digital camera are stored on a removable memory card in the camera. These memory cards often store up to 32 gigabytes of data, which provides enough space to store thousands of high-resolution photographs. Video camcorders, which once recorded video onto tapes or mini-CDs, now can save video footage in a digital format directly to a hard drive in the camera. The video files can be easily transferred from the camcorder to a computer.

41. A device known as a modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Electronic contact can be made to literally millions of computers around the world. The ability to produce child pornography easily, reproduce it inexpensively, and market it anonymously (through electronic communications) has drastically changed the method of distribution and receipt of child pornography. Child pornography can be transferred via electronic mail or through file transfer protocols (FTPs) to anyone with access to a computer and modem. Because of the proliferation of commercial services that provide electronic mail service, chat services (i.e., “Instant Messaging”), and easy access to the Internet, the computer is a preferred method of distribution and receipt of child pornographic materials.
42. The computer’s ability to store images in digital form makes the computer itself an ideal repository for child pornography. The size of the electronic storage media (commonly referred to as the hard drive) used in home computers has grown tremendously within the last several years. These drives can store thousands of images at very high resolution. In addition,

forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory “swap” or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.”

50. As further described in Attachment B, this application seeks permission to locate not only records that might serve as direct evidence of the crimes described in the warrant, but also for records that establish how computer systems were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any computer storage device on the SUBJECT PREMISES because:

- a. Virtual memory paging systems can leave traces of information on computer storage devices that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on computer storage devices that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other peripheral computer storage devices, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.
- b. As explained herein, information stored within a computer storage device may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element

or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer storage device (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculcating or exculpating the computer owner. Further, computer storage device activity can indicate how and when the computer or device was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, peripheral storage devices that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer system access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer storage device may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of

additional computer storage devices. The geographic and timeline information described herein may either inculcate or exculpate the computer user. Last, information stored within a computer storage device may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer storage device may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

- c. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a computer storage device that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer storage device and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.
- d. Further, in finding evidence of how a computer system was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a computer storage device. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

## **SPECIFICS OF SEARCH AND SEIZURE OF COMPUTER SYSTEMS**

51. Searches and seizures of evidence from computers commonly require agents to download or copy information from the computers and their components, or seize most or all computer items (computer hardware, computer software, and computer related documentation) to be processed later by a qualified computer expert in a laboratory or other controlled environment. This is almost always true because of the following two reasons
- a. Computer storage devices (like hard disks, diskettes, tapes, laser disks, magneto opticals, and others) can store the equivalent of thousands of pages of information. Rarely does all of this information take the form of documents and files that can be easily viewed on-site. Especially when the user wants to conceal criminal evidence, he or she often stores it in random order with deceptive file names. This requires searching authorities to examine all the stored data that is available in order to determine whether it is included in the warrant that authorizes the search. This sorting process can take days or weeks, depending on the volume of data stored, and is generally difficult to accomplish on-site in a non-intrusive and efficient manner.
  - b. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present at the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on-site. Further, the search of a computer system is an exacting procedure that is designed to protect the integrity of the evidence and to recover even hidden, erased, compressed,

password-protected, or encrypted files. Since computer evidence is extremely vulnerable to tampering or destruction (which may be caused by malicious code or normal activities of an operating system), the controlled environment of a laboratory is essential to its complete and accurate analysis. Taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

52. In order to fully retrieve data from a computer system, the analyst needs all magnetic storage devices as well as the central processing unit (“CPU”). In cases involving child pornography where the evidence consists partly of graphics files, the monitor(s) may be essential for a thorough and efficient search due to software and hardware configuration issues. In addition, the analyst needs all the system software (operating systems or interfaces, and hardware drivers) and any applications software which may have been used to create the data (whether stored on hard drives or on external media).
53. Furthermore, because there is probable cause to believe that the computer and its storage devices are all instrumentalities of crimes, within the meaning of 18 U.S.C. §§ 2252A(a)(5)(B) and (b)(2), they should all be seized as such.

#### **SEARCH METHODOLOGY TO BE EMPLOYED REGARDING ELECTRONIC DATA**

54. Based on the foregoing, and consistent with Federal Rule of Criminal Procedure 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying computer hardware, computer software, and/or memory storage devices, and would authorize a later review of the media or information consistent with the warrant. The search procedure of electronic data contained in computer hardware, computer software, and/or memory storage

devices may include the following techniques (the following is a non-exclusive list, as other search procedures may be used):

- a. on-site triage of computer systems to determine what, if any, peripheral devices or digital storage units have been connected to such computer systems, a preliminary scan of image files contained on such systems and digital storage devices to help identify any other relevant evidence or potential victims, and a scan for encryption software;
- b. on-site forensic imaging of any computers that may be partially or fully encrypted, in order to preserve unencrypted electronic data that may, if not immediately imaged on-scene, become encrypted and accordingly unavailable for examination; such imaging may require several hours to complete and require law enforcement agents to secure the search scene until that imaging can be completed;
- c. examination of all of the data contained in such computer hardware, computer software, or memory storage devices to view the data and determine whether that data falls within the items to be seized as set forth herein;
- d. searching for and attempting to recover any deleted, hidden, or encrypted data to determine whether that data falls within the list of items to be seized as set forth herein (any data that is encrypted and unreadable will not be returned unless law enforcement personnel have determined that the data is not (1) an instrumentality of the offenses, (2) a fruit of the criminal activity, (3) contraband, (4) otherwise unlawfully possessed, or (5) evidence of the offenses specified above);

- e. surveying various file directories and the individual files they contain;
- f. opening files in order to determine their contents;
- g. scanning storage areas;
- h. performing key word searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are likely to appear in the evidence described in Attachment B; and
- i. performing any other data analysis technique that may be necessary to locate and retrieve the evidence described in Attachment B.


#### **REQUEST FOR SEALING**

55. It is respectfully requested that this Court issue an order sealing, until further order of the Court, all papers submitted in support of this application, including the application and search warrant. I believe that sealing this document is necessary because the items and information to be seized are relevant to an ongoing investigation into a criminal organization and not all of the targets of this investigation will be searched at this time. Based upon my training and experience, I have learned that online criminals actively search for criminal affidavits and search warrants via the Internet, and disseminate them to other online criminals as they deem appropriate, i.e., post them publicly online through forums. Premature disclosure of the contents of this affidavit and related documents may have a significant and negative impact on the continuing investigation and may severely jeopardize its effectiveness. Further, this affidavit describes a law enforcement technique in sufficient detail that disclosure of this technique could assist others in thwarting its use in the future.

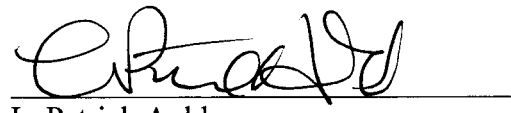


**CONCLUSION**

56. Based on the foregoing, there is probable cause to believe that the federal criminal statute cited herein has been violated, and that the contraband, property, evidence, fruits and instrumentalities of the offense, more fully described in Attachment B of this Affidavit, are located at the SUBJECT PREMISES, described in Attachment A. I respectfully request that this Court issue a search warrant for the SUBJECT PREMISES, authorizing the seizure and search of the items described in Attachment B.

  
Special Agent Tara S. Cataldo  
Federal Bureau of Investigation

Sworn to me this 15<sup>th</sup> day of October.

  
L. Patrick Auld  
United States Magistrate Judge

## **ATTACHMENT B**

### **PROPERTY TO BE SEIZED**

The following materials and records, which constitute evidence of the commission of a criminal offense, contraband, the fruits of crime, or property designed or intended for use or which is or has been used as the means of committing a criminal offense, namely violations of 18 U.S.C. §§ 2252A(a)(5)(B):

1. Computers or storage media used as a means to commit the violations described above.
2. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):
  - a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;
  - b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
  - c. evidence of the lack of such malicious software;
  - d. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;
  - e. evidence indicating the computer user's state of mind as it relates to the crime under investigation;
  - f. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;
  - g. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;

- h. evidence of the times the COMPUTER was used;
  - i. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;
  - j. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;
  - k. records of or information about Internet Protocol addresses used by the COMPUTER;
  - l. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses; and
  - m. contextual information necessary to understand the evidence described in this attachment.
3. Routers, modems, and network equipment used to connect computers to the Internet.
4. Records, information, and items relating to violations of the statutes described above in the form of:
- a. records and information constituting child pornography, as defined in 18 U.S.C. 2256(8);
  - b. records and information constituting child erotica;
  - c. records and information revealing sexual activity with or sexual interest in minors;
  - d. records or information constituting or revealing the receipt, distribution, or production of child pornography;
  - e. records and information revealing the identity or location of the persons suspected of violating the statute described above and items revealing the ownership or use of computer equipment found in the above residence;
  - f. records and information revealing sexual exploitation of children, including correspondence and communications between users of "Website A";
  - g. records and information revealing the use of "Website A" and the "the Network";

- h. records and information constituting or revealing personal identifying information or contact information of individuals who were contacted for the purpose of committing violations of the statute described above;
- i. records and information constituting or revealing membership or participation in groups or services that provide or make accessible child pornography;
- j. records and information revealing accounts with any internet service provider;
- k. records and information revealing the use and identification of remote computing services such as email accounts or cloud storage;
- l. records and information constituting and revealing malicious software; and
- m. records and information revealing the ownership, occupancy, or possession of 112 Odell Place, Apartment 4, Greensboro, North Carolina 27403, and a Toyota Yaris vehicle bearing North Carolina license plate ZYD5374 and Vehicle Identification Number JTDKT903095263488.

5. During the course of the search, photographs of the searched premises may be taken to record the condition thereof and/or the location of items therein.

As used above, the terms “records” and “information” includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term “computer” means an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term “storage medium” means any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.